PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-177696
(43)Date of publication of application : 04.08.1987

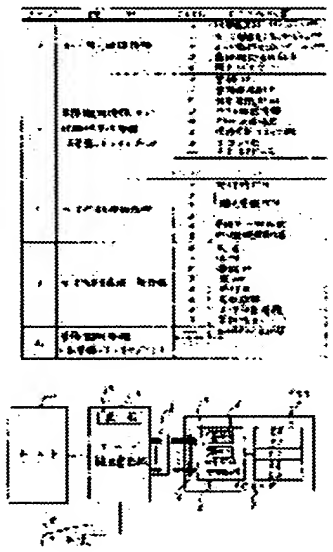
(51)Int.Cl. G06K 19/00
B42D 15/02

(21)Application number : 61-018040
(22)Date of filing : 31.01.1986

(71)Applicant : HITACHI LTD
(72)Inventor : YAMASHITA KOTARO
KAWAOKA AKIHIRO
ASAMI KO

(54) MULTI-PURPOSE IC CARD AND METHOD TO USE

(57)Abstract:
PURPOSE: To apply a single IC card to plural works by comparing the collating result of identifying information and access conditions based on the contents of respective areas set to a memory and determining the permission or the rejection of an access request to the memory.
CONSTITUTION: In a memory 3 of an IC card 1, zones Z0WZ4 are included, and in respective zones, the information shown in the figure is stored. By a microprocessor 2, first, card identity confirming information sent from a card reading writing machine 7 is compared with the corresponding information in the card, and at the time of coincidence, the corresponding flag of a permission flag table 5 is set to '1'. Next, work identifying information is compared with corresponding information, and at the time of coincidence, the corresponding flag of the table 5 is set to '1'. Next, inputted identifying information PIN is coincident to a PIN in the memory, and then, the flag of a permission flag table 4 is set to '1'. Next, when an access request is executed, tables 4 and 5 are compared, the permission or the rejection of the request access action are investigated and in accordance with the result, execution or rejection is performed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－177696

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和62年(1987)8月4日
G 06 K 19/00		N－6711－5B	
B 42 D 15/02		7008－2C	
G 06 K 19/00		Q－6711－5B	審査請求　未請求　発明の数 2　（全9頁）

㊹発明の名称　多目的ＩＣカード及びその使用方法

㉑特　願　昭61－18040

㉒出　願　昭61(1986)1月31日

㉒発　明　者　山下　廣太郎　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉒発　明　者　川岡　明宏　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉒発　明　者　浅見　香　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉑出　願　人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地

㉔代　理　人　弁理士　野萩　守　外1名

明　細　書

1. 発明の名称

多目的ＩＣカード及びその使用方法

2. 特許請求の範囲

1. マイクロプロセッサと前記マイクロプロセッサを介して外部からアクセス可能なメモリとを内蔵し、業務の履行に際して前記メモリへのアクセスが必要とされるカードにおいて、前記メモリは、登録された各業務に関する識別情報のための領域と、前記各業務の個別情報のための領域と、各業務の前記個別情報領域を規定する領域管理情報のための領域とを含むことを特徴とする、多目的ＩＣカード。

2. 特許請求の範囲1において、前記領域管理情報は、各業務の個別情報領域の位置を示す情報と大きさを示す情報とを含む、多目的ＩＣカード。

3. 特許請求の範囲1において、前記識別情報領域と領域管理情報領域は空き領域の一方の端から始まり、前記個別情報領域は空き領域の他端から始まる。多目的ＩＣカード。

4. 特許請求の範囲1において、前記メモリ内の情報の各項目は、前記マイクロプロセッサにより実アドレスに変換される統一的形式の論理アドレスを持つ、多目的ＩＣカード。

5. 特許請求の範囲1において、前記メモリ内の情報へのアクセスの許可条件が各項目に対して別個に定められた、多目的ＩＣカード。

6. マイクロプロセッサと前記マイクロプロセッサを介して外部からアクセス可能なメモリとを内蔵し、前記メモリが、登録された各業務に関する識別情報のための領域と、前記各業務の個別情報のための領域と、各業務の前記個別情報領域を規定する領域管理情報のための領域とを含む、多目的ＩＣカードを使用して業務を履行する際に行なわれる、所定の識別情報を外部機器から前記マイクロプロセッサに入力するステップと、前記マイクロプロセッサにおいて前記入力識別情報とそれに対応する前記メモリ内の

識別情報とを照合してその結果を保持するステップと、前記メモリ内の情報のある項目へのアクセス要求を前記外部機器から前記マイクロプロセッサに入力するステップと、前記マイクロプロセッサにおいて前記メモリ内の情報の各項目につき予め定められたアクセス許可条件と前記照合結果とを比較して前記アクセス要求の許否を決定するステップとを含むことを特徴とする、多目的ＩＣカードの使用方法。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、ＩＣカードに関し、特に、複数の目的又は業務（身分証明、入場管理、銀行取引、クレジット購買等）に共用されるＩＣカードと、その使用方法に関する。

〔従来の技術〕

ＩＣカードに関しては、特公昭５３－６４９１号以下多くの発明や提案があるが、カードの利用態様については、マイクロプロセッサのデータ処理機能を利用する本人確認行為の域を出ないものがほとんどである。また、適用業務に関しても、単一の業務への適用が主であって、複数の業務、特に、記録される情報の形態、アクセス条件などを異にする複数の業務での共用に対しては、特段の工夫がなされたようには見受けられない。

〔発明が解決しようとする問題点〕

１枚のカードを複数の業務に対して共用する場合に、権限チェックが各業務に独自の情報に基づいて行なえることが望ましい。ある一組の条件に関する権限チェックですべての業務における権限を認める方法では、適用業務の範囲に著しい制限を課さざるをえない。また、記録される情報の形式や長さも、一般に、業務によって大幅に異なるから、これらについての制約があったり、あるいは、その制約を除くために特殊な処理を必要とするのでは、至って不便である。更に、適用業務の個数も、メモリ容量の許す限り多いことが望ましい。単一のＩＣカードに複数の業務を登録するための常識的な方法は、メモリをいくつかの固定長領域に分割して、各領域を一つの業務に割当てることである。しかし、この方法では、メモリ領域のむだが多く、予め定められた個数を越えた業務は、たとえ空き領域の総和が充分な容量に達していても、登録することができない。

本発明は、前記の問題を解決し、それにより、権限チェック条件、記録情報の形式と長さなどが大幅に異なる可及的多数の業務に共用しうる、多目的ＩＣカードを提供しようとするものである。

〔問題点を解決するための手段〕

本発明によるＩＣカード内のメモリは、特徴として、各業務に関する識別情報（例えば、業務識別コード、業務個有の顧客識別番号等）のための領域と、各業務の個別情報（例えば、取引履歴、特定業務専用の顧客管理情報等）のための領域と、各業務の個別情報領域を規定する領域管理情報（例えば、各領域の位置、大きさ等）のための領域とを含む。

また、前記ＩＣカードの使用方法は、特徴として、入力された識別情報とそれに対応するメモリ内識別情報を照合してその結果を保持するステップと、メモリ内情報の各項目につき予め定められたアクセス許可条件と前記照合結果を比較してメモリ内情報へのアクセス要求の許否を決定するステップとを含む。

〔作用〕

別個に記憶された各業務に関する識別情報は、個別の識別情報に基づく業務ごとの権限チェックを可能にする。また、各業務の個別情報領域に対する領域管理情報を利用することにより、長さや形式の異なる複数の業務の個別情報を、メモリ領域のむだなく密に配置することができ、したがって、メモリ容量の許す限り多数の業務を登録することができ、新業務の追加も容易である。更に、業務により長さや形式の異なる業務個別情報へのアクセスを、領域管理情報を用いるアドレス変換を介して、統一的な論理アドレスによって指定することができる。

また、カード使用に際して、識別情報入力とメモリ内の対応識別情報の照合結果を保持するステップにより、チェックを要する諸識別項目につい

ての合否のテーブルが形成され、この照合結果とメモリ内情報の各項目につき予め定められたアクセス許可条件とを比較してアクセス要求の許否を決定するステップにより、項目及びアクセス形態ごとに異なるアクセス権限の有無が、アクセス要求の都度個別にチエックされる。

〔実施例〕

本発明のＩＣカードは、ＬＳＩとして形成されたマイクロプロセッサと不揮発性メモリ（例えば、ＥＥＰＲＯＭ）を内蔵する。第１図はそのメモリに記憶される情報の一例を示す。メモリ内の情報は多数のアイテムからなり、これらのアイテムはいくつかのゾーンにまとめられる。

ゾーン０の内容は、カード身元確認情報であり、主にカードの正当性のチエックに用いられる。アイテム０はＩＣ製造元ＩＤ（ＩＤは識別情報の略語）と当該ＩＣのバージョン番号であり、アイテム１はカード製造元ＩＤと当該カードの製造バージョン番号であり、アイテム２はカード発行元ＩＤと当該カードの発行バージョン番号であり、アイテム３は最終確認責任者ＩＤであり、アイテム４は最終確認責任者のパスワードである。ＩＣチップの作製時に、~~半導体~~ＩＣ製造元ＩＤとバージョン番号（アイテム０）と、ＩＣ製造元における最終確認責任者ＩＤとそのパスワード（アイテム３，４）が書込まれる。次に、カードの作製時に、カード製造元ＩＤとバージョン番号（アイテム１）が書込まれるとともに、アイテム３と４は、カード製造元における最終確認責任者ＩＤとそのパスワードにそれぞれ書替えられる。最後に、カードの発行時に、カード発行元ＩＤとバージョン番号（アイテム２）が書込まれるとともに、アイテム３と４は、カード発行元における最終確認責任者ＩＤとそのパスワードにそれぞれ書替えられる。

ゾーン１は、取扱う業務にそれぞれ対応するいくつかのサブゾーンからなる。各サブゾーンの内容は、対応する業務についての業務識別情報と記録域管理情報からなり、業務識別情報は主に当該業務の履行権限のチエックに用いられ、記録域管理情報は対応する業務の個別情報（後述するゾーン４）のためのメモリ領域の管理に用いられる。アイテム０は業務ＩＤであり、アイテム１は業務権限者ＩＤである。業務は、例えば、特定銀行との取引、特定店での購買、特定地区への入出、特定機器の操作、特定サービスの享受などであり、業務権限者は、関連する特定の銀行、店、地区又は機器の管理者、サービス提供者などである。アイテム２の利用者識別番号は、各業務についてカード所有者に与えられた個有の識別情報で、例えば、銀行口座番号、顧客番号などである。アイテム３のホスト返送情報は、カード内情報の処理の開始が外部機器（カード読出書込装置又はホスト処理装置）から要求された時に、リターン情報として送出される情報であり、その内容は業務により異なる。アイテム４のＰＩＮ必須指定は、後述するゾーン４へのアクセスに対して、ＰＩＮ（後述するゾーン２に書込まれる本人確認用暗証コード）の一致を必須条件とするか否かを指定する情報である。アイテム５は、後述するゾーン４内で当該業務のために使用しうるブロックの個数であり、アイテム６はそのブロックの長さ（例えば、バイト数）である。これらのアイテムの他に、ゾーン１は、前述の使用しうるブロックのスタートアドレスを含む。スタートアドレスは、内蔵マイクロプロセッサにとってのみ意味がある内部管理情報であるから、アイテム番号を持たない。ゾーン１の情報は、それぞれの適用業務の登録時に書込まれる。

ゾーン２の内容は、カード所有者確認情報であり、主に本人の確認のために用いられる。アイテム０はカード発行時に一応与えられるＰＩＮ（本人確認用暗証番号：Personal Identification Number）であり、アイテム１～３はその後各人が任意に決定して書込むＰＩＮである。各ＰＩＮは、例えば、４～１０桁の１０進数である。アイテム４は記憶されたＰＩＮと入力されたＰＩＮの不一致の累積数である。この情報は、例えば、後述するカードの有効性の決定に用いることができる。アイテム５は同一のＰＩＮの連続使用の可否を指定する情報であり、それは、ＰＩＮの連続使

用の可否を示すビットと、各ＰＩＮが前回使用された結果一時的に無効にされているか否かを示すビット群を含む。同一ＰＩＮの連続使用の拒否が指定されると、たとえ正しいＰＩＮであっても、同じＰＩＮを続けて入力したときには、ＰＩＮの不一致として扱われる。この指定により、あるＰＩＮを他人に知られたときでもカードの盗用を防止することができる。アイテム０と５はカードの発行時に書込まれる。

ゾーン３は、カード所有者属性一般情報であり、全業務で共通に必要とされる範囲の属性情報と、カードシステムの運用上必要な情報からなる。アイテム０は氏名、アイテム１は住所、アイテム２は電話番号、アイテム３はカードシステムでの客番号、アイテム４はカードの発行日、アイテム５はカードの有効期限である。アイテム６はユーザ（カード発行元）が必要に応じて書込む任意の情報である。アイテム７はカードの有効性を示す情報であって、例えば、ゾーン２のアイテム４に記録された累積不一致回数が所定値に達したときに、カードが無効であることを示すように書替えられる。このゾーンはカードの発行時に書込まれ、アイテム６は当初は有効を示すコードである。

ゾーン４は、ゾーン１に登録されたそれぞれの業務に対応するサブゾーンからなり、各サブゾーンの内容は、対応する業務の個別情報、例えば、従来の磁気カードの記録情報、取引履歴、預金残高、非公開の顧客管理情報（勤務先、職位、年俸、資産等）、暗号キーなどであり、その性質により、業務登録時のまま固定され、あるいは、カードの使用の都度書込まれ又は更新される。このゾーンの情報は、ブロックと呼ばれる格納領域を単位としてアクセスされる。各業務における使用可能ブロック数及びブロック長はゾーン１のアイテム５及び６によりそれぞれ指定され、これら一連のブロックのスタートアドレスはゾーン１に管理情報として含まれている。各業務のための一連のブロックには、それぞれのＢＳＮ（Block Serial Number）が付与される。

メモリ内の情報は、対外的には、ゾーン番号とアイテム番号又はゾーン番号とＢＳＮからなる統一的な論理アドレスによって識別される。ゾーン０、２及び３の各アイテムは、固定長であり、予め定められたそれぞれのメモリ領域に格納される。ゾーン１は、全体としては可変長であるけれども、各アイテム、したがって各サブゾーンは固定長であるから、業務ＩＤを指定してサーチすることができる。ゾーン４のデータは、格納位置、データ長等が業務によって異なるけれども、ＢＳＮが与えられれば、ゾーン１中のスタートアドレスとブロック長情報を用いて、指定されたブロックの実アドレスを決定することができる。論理アドレスから実アドレスへの変換は、内蔵マイクロプロセッサにより遂行される。

ゾーンとアイテムのメモリ内配置は、必ずしも第１図に示されたような整然としたものである必要はなく、一定のアルゴリズム又はテーブルに従って分散することにより、機密保護性を高めることができる。同じ目的で、記憶される情報にもシャフル等の加工を施すことができる。長さが不定のゾーン１及び４については、空きメモリ領域をその両端から順次各業務に割当てるのがよい。例えば、ゾーン１のサブゾーンには空き領域の先頭部分を割当て、ゾーン４のサブゾーンには空き領域の末尾部分を割当てる。あるいは、この逆でもよい。この割当アルゴリズムによれば、ゾーン１とゾーン４のためのそれぞれの領域を予め区分する必要がなく、メモリ容量の許す限り、任意の数の適用業務を登録又は追加することができる。

各ゾーンの各アイテムへのアクセス（読出し、書込み、消去）の許可条件は、各アイテムごとに、かつ、読出し、書込み、消去のそれぞれに対して、条件テーブルの形で任意に設定することができる。第２図は条件テーブルの一例を示す。図において、「読出」、「書込」、「消去」の各欄における０個ないて４個は、一致チェック項目を示し、０個はゾーン０のアイテム３「最終確認責任者ＩＤ」、１個は同ゾーンのアイテム４「最終確認責任者パスワード」、２個はゾーン１のアイテム０「業務ＩＤ」、３個は同ゾーンのアイテム１「業務権限

者ＩＤ」、４個はゾーン２のアイテム０～３のいずれか一つのＰＩＮに、それぞれ対応する（第５図参照）。これらの欄に記入された○印は、当該チエック項目の一致が対応アイテムへのアクセスの条件として設定されていることを表わす。同一アイテムに対する複数の○印は、それらのチエック項目の論理和がアクセス条件となることを示す。例えば、ゾーン０のアイテム０～２の読出しは、最終確認責任者ＩＤ又は同パスワードの一方が一致すれば可能であるが、同ゾーンのアイテム３の読出しは、最終確認責任者パスワードが一致した場合にのみ可能であり、同ゾーンのアイテム４の読出しは不可能である。ゾーン０の消去は、カード発行後は不可能である。ゾーン４に対するアクセス条件欄中の△印は、そのチエック項目の一致によるアクセス許可が、ゾーン１のアイテム４においてＰＩＮ必須指定がなされていない場合にのみ有効になることを表わす。このような条件テーブルは、内蔵マイクロプロセッサ内のＲＯＭ又はメモリ中の特定領域に、ＩＣの製造時に書込まれる。

第３図は、本発明のＩＣカードとそのための処理システムを模式的に示す。ＩＣカード１は、マイクロプロセッサ２と、それに接続された不揮発性メモリ（例えば、ＥＥＰＲＯＭ）３とを内蔵する。マイクロプロセッサ２は、前述の条件テーブル（第２図）４と、後述する認可フラグテーブル（第５図）５とを備える。ＩＣカードの使用にあたり、マイクロプロセッサの端子ピン６は、カード読出書込機７のソケット８に挿入される。カード読出書込機７は、ＰＩＮその他の情報を入力するためのキーボード９と、ガイダンスその他の情報を表示するための表示装置１０を有する。業務によっては、カード読出書込機１０はホストコンピュータ１１に接続されてもよい。

カード読出書込機７又はホストコンピュータ１１とＩＣカード内のマイクロプロセッサ２の間で伝送されるコマンド及びデータは、すべての処理について、第４図に示されるフォーマットのメッセージの形をとる。第４図において、ＦＨはメッセージの先頭を示すフィールドヘッダ、Ｃはコマンド、Ｚはゾーン番号、ｉ又はＢＳＮはアイテム番号又はＢＳＮ、ＢＣＣはブロックチエックコード、ＦＥはメッセージの末尾を示すフィールドエンドコードである。ｉ又はＢＳＮのフィールドに空白コードがセットされたときは、ゾーン又はサブゾーンの全体が指定されたものと解釈される。

カード１がソケット８に挿入されて処理が開始されると、ホストコンピュータ１１又はカード読出書込機７から送られた適当なコマンドに従い、第２図に示された条件テーブル上の各チエック項目０～４が一致するか否かが、マイクロプロセッサ２によりチエックされ、その結果が、認可フラグテーブル５に書込まれる。第５図は、認可フラグテーブル５の内容の一例を示す。最終確認責任者ＩＤとそのパスワード、適用業務に対する業務ＩＤと業務権限者ＩＤ、又はＰＩＮが一致すれば、対応する位置０～４の認可フラグが“１”にセットされる。認可フラグテーブルの内容は、メモリ内の情報へのアクセス要求の許否を決定する時に条件テーブルの内容と比較される。

第６図は、アクセス要求の許否を決定するためにマイクロプロセッサ２が遂行する処理のフローチャートである。カードがソケット８に挿入された後、カード読出書込機７又はホストコンピュータ１１からの初期化コマンドを受けて、マイクロプロセッサ２による処理が開始される。まず、カード読出書込機７から送られたカード身元確認情報（例えば、最終確認責任者ＩＤ及び／又はパスワード）がカード内の対応情報と比較され、一致すれば、認可フラグテーブル５の対応フラグ（０，１）が“１”にセットされる（２１）。カード身元確認情報は、カード読出書込機７又はホスト１１に予め固定的にセットされていてもよい。他の方法として、メモリ３内のゾーン１のアイテム３～４の内容に一定の相互関係を持たせておき、その関係が充たされているか否かを、マイクロプロセッサ２の内部処理のみによってチエックしてもよい。以後、この形のチエックを内部チエックと呼ぶ。

次に、カード脱出書込機７又はホストコンピュータ１１から送られた業務識別情報（例えば、業務ＩＤ及び／又は業務権限者ＩＤ）がカード内の対応情報と比較され、一致すれば、認可フラグテーブルの対応フラグ（２，３）が"１"にセットされる（２２）。業務識別情報も、カード脱出書込機７又はホスト１１に固定的にセットされていてもよい。

履行しようとしている業務に対してＰＩＮ必須指定（ゾーン１のアイテム４）が設定されていれば、次に本人チェック（２３）が行なわれる。すなわち、キーボード９から入力されたＰＩＮが、ゾーン２のアイテム０～３のＰＩＮのどれかと一致するか否かが調べられる。この時、ゾーン２のアイテム５が調べられ、ＰＩＮの連続使用が許されていない場合には、入力されたＰＩＮがその時点で無効にされているか否かも併せて調べられる。その結果、入力されたＰＩＮとメモリ内の有効なＰＩＮの一つが一致すれば、認可フラグテーブルの位置４のフラグが"１"にセットされる。

その後、カード脱出書込機７又はホストコンピュータ１１からメモリ内情報に対するアクセス（読出し、書込み、消去）を要求するコマンドが送られると、マイクロプロセッサ２は、条件テーブル４と認可フラグテーブル５を比較して、対象アイテムに対して要求されたアクセス動作（読出し、書込み、消去）が許容しうるか否かを調べ（２４）、その結果に従って、要求されたアクセスを実行し（２５）、あるいは拒否する（２６）。

次に、前述のＩＣカードが銀行預金業務と健康管理業務に適用された場合について、コマンドに従ったカード処理過程の例を説明する。ただし、カードの正当性のチェックは、適用業務設定過程を除き、カードの挿入により自動的に起動される前述の内部チェックにより果たされるものとし、かつ、次のコマンドが用意されているものとする。

ＩＮＴ：

これは、ＩＣカードとの会話の開始を宣言する初期化コマンドであり、カード身元確認情報又は業務識別情報とホスト返送情報の要否を示す情報とを、メッセージのデータ部に含む。これを受けたカード内マイクロプロセッサは、カードの正当性又は業務の適用性のチェック（第６図２１又は２２）を行なうとともに、ホスト返送情報（ゾーン１のアイテム３）を要求に応じて返送する。

ＣＨＫ：

これは、識別情報（業務ＩＤ、ＰＩＮ等）をデータ部に含み、それとメモリ内の指定されたアイテムとの一致性のチェックを要求する。ただし、ゾーン１及び５については、業務ＩＤの一致が確認された後の当該業務のサブゾーンのみがチェックの対象となる。

ＷＲＴ：

これは、データ部の内容のメモリへの書込みを要求する。

ＲＤＤ：

これは、メモリ内の情報の読出しを要求する。

以下の説明において、コマンド略号に続く括弧内の語は、メッセージのゾーン番号部、アイテム番号又はＢＳＮ部、及びデータ部の各内容を示す。記号"Ｚ"はゾーン、"ｉ"はアイテム、"－"は空白、"Ａ"はカード発行元（ＶＡＮ業者）の最終確認責任者、"Ｂ"は銀行預金業務、"Ｃ"は健康管理業務を、それぞれ表わす。また、条件テーブルは第２図のように設定されているとする。

適用業務Ｂ及びＣの登録は、次のようなコマンド列によって行なわれる。カード身元確認情報（ゾーン０）は既に書込まれているとする。

(1)　ＩＮＴ（Ｚ０，ｉ４，Ａのパスワード）

このコマンドにより、カードとの会話が開始され、同時に、入力されたＡのパスワードとゾーン０のアイテム４との一致性がチェックされ、その結果に従って、認可フラグ１がセットされる。ホスト返送情報は要求されない。

(2)　ＷＲＴ（Ｚ１，－，ＢのＺ１情報）

アイテム番号は指定されず、データ部の内容は銀行預金業務に対してゾーン１に設定すべき全アイテムであり、これらを一つのサブゾーンとして書込まれる。ホスト返送情報（ｉ３）と

して口座番号と暗証番号と次に書込むべきブロックのＢＳＮとが指定され、ＰＩＮ必須指定（ｉ４）がセットされ、使用可能ブロック数（ｉ５）は"１０"、ブロック長（ｉ６）は３２バイトであるとする。

(3) ＷＲＴ（Ｚ１，－，ＣのＺ１情報）

このコマンドにより、前記と同様にして、健康管理業務に対するゾーン１の全アイテムが書込まれる。ホスト返送情報は空白であり、ＰＩＮ必須指定はなく、使用可能ブロック数は"１"で、ブロック長は５６バイトとする。

銀行預金業務における取引に係してのコマンドシーケンスは、例えば、次のとおりである。

(1) ＩＮＴ（Ｚ１，ｉ０，ＢのＩＤ・ホスト返送情報要求）

このコマンドにより、業務の適用性のチェック（第６図２２）が業務ＩＤについて行なわれ一致すれば、認可フラグ２がセットされるとともに、ホスト返送情報として、口座番号と暗証番号と次に書込むべきブロックのＢＳＮとが、

カード読出書込機７に送られる。なお、カード正当性チェックは、前述のように、自動内部チェックにより完了している。

(2) ＰＩＮの入力

ＰＩＮの入力を促すガイダンスが表示され、カード使用者は、キーボード９を用いて、ＰＩＮを入力する。

(3) ＣＨＫ（Ｚ２，－，ＰＩＮ）

このコマンドにより、本人チェック（第６図２３）が行なわれ、入力されたＰＩＮとメモリ内のＰＩＮのどれかが一致すれば、認可フラグ４がセットされる。その後、

(4) ＷＲＴ（Ｚ４，ＢＳＮ，取引データ）

このコマンドにより、取引（預金引出し、入金等）に関するデータが、ホスト返送情報により指定されたＢＳＮを持つブロックに書込まれる。

(5) ＷＲＴ（Ｚ１，ｉ３，更新されたＢＳＮを含む新ホスト返送情報）

このコマンドにより、次に書込むべきブロックを示すＢＳＮを含む更新されたホスト返送情報が、ゾーン１のアイテム３としてセットされる。

次に、健康管理業務における情報読出しのためのコマンドシーケンスの例を示す。

(1) ＩＮＴ（Ｚ１，ｉ１，$^{C}_{K}$のＩＤ）

このコマンドにより、業務ＩＤがチェックされ、一致すれば認可フラグ２がセットされる。ホスト返送情報は用意されていない。カード正当性チェックは自動内部チェックにより完了している。

(2) ＲＤＤ（Ｚ４，－，－）

健康管理業務のためのゾーン４は単一のブロックからなるので、ＢＳＮを指定する必要はない。ＰＩＮ必須指定はセットされていなかったから、ＩＮＴコマンドに応じて行なわれた業務ＩＤのチェックにより認可フラグ２がセットされていさえすれば、健康管理に関するゾーン４の情報（病歴、医学的特徴等）を読出すことができる（第２図△印参照）。

条件テーブル及び認可フラグテーブルの内容は、第２図及び第５図に示されたものに限られず、任意のチェック項目の組合せを指定してよい。チェック項目間の論理関係も、論理和に限られず、他の所要の論理結合を採用してよい。

〔発明の効果〕

本発明によれば、各業務に対する権限チェックを個別に行なうことができ、また、データの形式や長さの異なる多種多様な業務に関する情報をメモリ容量のむだなく記録することができ、かつ、すべての情報へのアクセスを統一的な論理アドレスを用いて行うことができる。したがって、単一ＩＣカードの複数業務への適用が容易になる。

4. 図面の簡単な説明

第１図は本発明によるＩＣカード内のメモリの内容の一例を示す図、第２図は第１図に示されたメモリ内容へのアクセス許可条件を定める条件テーブルの一例を示す図、第３図は本発明によるＩＣカード及びそれが適用されるカード処理システムのブロックダイヤグラム、第４図はカード内の

マイクロプロセッサと外部機器の間で伝送されるコマンドのフォーマット図、第５図は識別情報の照合の結果形成される認可フラグテーブルの一例を示す図、第６図はカード内のマイクロプロセッサによるアクセス許否決定処理のフローチャートである。

１…ＩＣカード、２…マイクロプロセッサ、３…メモリ、Ｚ０～Ｚ４…情報ゾーン、４…発行テーブル、５…認可フラグテーブル、７…カード読出書込機、９…キーボード、１１…ホストコンピュータ。

代理人　弁理士　野　祇　　守
（他か１名）

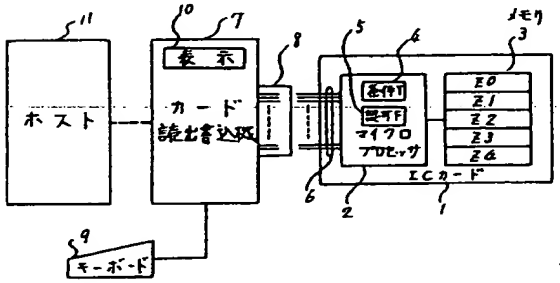
第１図

ゾーン	種　別	アイテム	アイテム内容
0	カード多元確認情報	0	IC製造元ID、バージョンNO
		1	カード製造元ID、バージョンNO
		2	カード発行元ID、バージョンNO
		3	最終確認責任者ID
		4	同上パスワード
1	業務識別情報 及び記録域管理情報（各業務ごとにサブゾーン）	0	業務ID
		1	業務権限者ID
		2	利用者識別NO
		3	ホスト返送情報
		4	PIN使用指定
		5	使用可能ブロック数
		6	ブロック長
		—	スタートアドレス
		⋮	⋮
2	カード所有者確認情報	0	発行時PIN
		1	
		2	個人登録PIN
		3	
		4	累積不一致回数
		5	PIN連続使用可否
3	カード所有者属性一般情報	0	氏名
		1	住所
		2	電話NO
		3	客NO
		4	発行日
		5	有効期限
		6	ユーザ任意情報
		7	有効性コード
4	業務個別情報（各業務ごとにサブゾーン）	—	BSN0～BSNL
		⋮	⋮

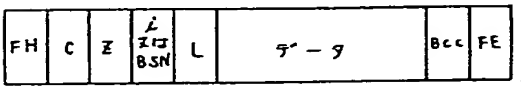
第２図

ゾーン	アイテムNo	アイテム内容	読出 0 1 2 3 4	書込 0 1 2 3 4	列在 0 1 2 3 4
0	0	IC製造元ID、バージョンNO	○ ○		
	1	カード製造元ID、バージョンNO	○ ○	○	
	2	カード発行元ID、バージョンNO	○ ○	○	
	3	最終確認責任者ID	○	○	
	4	同上パスワード		○	
1	0	業務ID	○ ○	○	○
	1	業務権限者ID	○ ○	○ ○	
	2	利用者識別NO	○ ○ ○	○ ○	
	3	ホスト返送情報	○ ○	○ ○	
	4	PIN使用指定	○ ○	○	
	5	使用可能ブロック数	○ ○	○	
	6	ブロック長	○ ○	○	
	—	スタートアドレス			
2	0	発行時PIN	○	○	○
	1	個人登録PIN	○	○	○
	2	〃	○	○	○
	3	〃	○	○	○
	4	累積不一致回数	○ ○	○	○
	5	PIN連続使用可否	○ ○	○	
3	0	氏名	○ ○ ○	○	○
	1	住所	○ ○ ○	○	○
	2	電話NO	○ ○ ○	○	○
	3	客NO	○ ○ ○	○	○
	4	発行日	○ ○ ○	○	○
	5	有効期限	○ ○ ○	○	○
	6	ユーザ任意情報	○ ○ ○	○	○
	7	有効性コード	○ ○ ○	○	○
4	—	BSN0～BSNL	△ ○	△ ○	△ ○
		BSN0～BSNj	△ ○	△ ○	△ ○

第３図



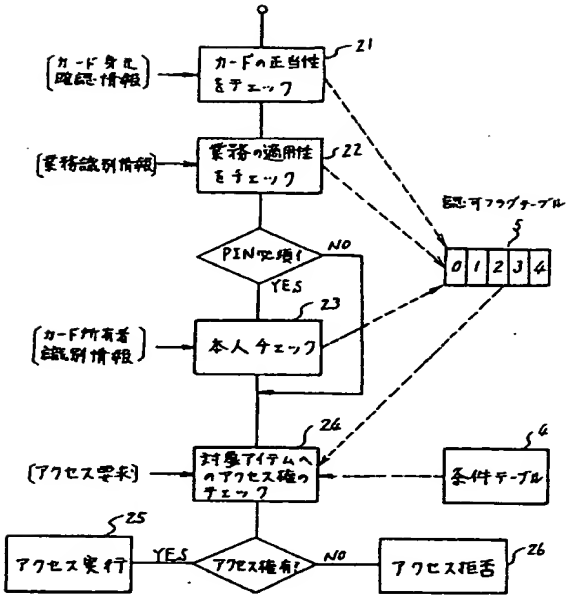
第４図



第５図

	最終確認責任者		適用業務		PIN
	ID	パスワード	業務ID	業務権限者ID	
フラグ位置	0	1	2	3	4

第６図


カード有効確認情報
カードの正当性をチェック
21
業務識別情報
業務の適用性をチェック
22
認可フラグテーブル
5
PIN必須?
NO
YES
0 1 2 3 4
23
カード所有者識別情報
本人チェック
24
アクセス要求
対象アイテムへのアクセス権のチェック
6
条件テーブル
25
アクセス実行
YES
アクセス権有?
NO
アクセス拒否
26